

**REMARKS**

Initially, in the Office Action dated February 11, 2004, the Examiner rejects claims 1-17 under 35 U.S.C. §103(a) as being unpatentable over RFC 2402, 2367, 2407, 2401 and 2409 and "ISO Authentication Framework", p. 574-577 (Schneier).

By the present response, Applicants have amended claims 1 and 7 to further clarify the invention. Claims 1-17 remain pending in the present application.

**35 U.S.C. §103 Rejections**

Claims 1-17 have been rejected under 35 U.S.C. §103(a) as being unpatentable over RFC 2402, 2367, 2407, 2401 and 2409 and Schneier. Applicants respectfully traverse these rejections.

RFC (Request for Comments) 2402 is entitled "IP Authentication Header" and merely discloses details regarding the IP authentication header including the header format, header processing, auditing, conformance requirements, security considerations, etc.

RFC 2367 is entitled "PF\_KEY Key Management API, Version 2" and discloses a generic key management API that can be used not only for IP Security but also for other network security services.

RFC 2407 is entitled "The Internet IP Security Domain of Interpretation for ISAKMP" and discloses a framework for security association management and cryptographic key establishment for the Internet. This framework consists of defined exchanges, payloads and processing guidelines that occur within a given domain of interpretation (DOI). This document defines the Internet IP security domain of

interpretation which instantiates ISAKMP for use with IP when IP uses ISAKMP to negotiate security associations.

RFC 2401 is entitled "Security Architecture for the Internet Protocol" and discloses the base architecture for IPsec compliant systems. This includes the goals of such systems, their components and how they fit together with each other and into the IP environment as well as the security services offered by the IPsec protocols, and how these services can be employed in the IP environment.

RFC 2409 is entitled "The Internet Key Exchange (IKE)" and discloses a protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI.

Schneier merely discloses details regarding the ISO authentication framework, also known as the X.509 protocol. The framework provides for authentication across networks. The X.509 protocol specification recommends RSA for security or authentication and has provisions for multiple algorithms and hash functions.

Regarding claims 1 and 12, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of these claims of, inter alia, obtaining first and second certificates from a certificate authority, using a certificate authority certificate, first certificate and private key with IKE to generate a WLAN link level key and mutually authenticating the mobile terminal and the access point using

the IKE, using a certificate authority certificate, second certificate and private key with IKE to generate IPsec authentication, encryption and decryption keys for data packets transferred between the mobile terminal and the server, generating an IPsec authentication header in a mobile terminal, or including the IPsec authentication header in a MAC-level message transferred from the mobile terminal to an associated access point. The Examiner asserts that RFC 2402, 2367, 2407, 2401, 2409 disclose all the limitations of claim 1 but provides no specific details associating each limitation in the claims of the present application with any portion of any of these disclosures. The Examiner simply makes a conclusory statement and provides no details supporting these assertions.

The Examiner admits that none of the RFC documents disclose or suggest a wireless local area network (WLAN) having a mobile terminal access point and a server and associating the mobile terminal with the access point, or obtaining first and second certificates from a certificate authority and using them to generate the WLAN link level key and generate IPsec authentication, but asserts that Schneier discloses these limitations on pages 576-577. However, this portion of Schneier merely discloses details regarding authentication protocols using illustrative examples where Alice wants to communicate with Bob and goes to a database and obtains a certification path from Alice to Bob and Bob's public key. Alice can now initiate either a one-way, two-way or three-way authentication protocol. An example sequence for each protocol is disclosed. However, these portions of Schneier do not disclose or suggest anything related to key generation. Specifically, these portions

of Schneier do not disclose or suggest using a certificate authority certificate, first certificate and a private key with IKE to generate a WLAN link level key, or using a certificate authority certificate, second certificate and private key with IKE to generate IPsec authentication, encryption and decryption keys for data packets transferred between a mobile terminal and a server. Just as the title suggests, Schneier relates to authentication. Schneier does not disclose or suggest anything related to encryption keys being generated, as recited in the claims of the present application. Further, Schneier does not disclose or suggest a mobile terminal or a server. The Examiner uses impermissible hindsight in reading the limitations in the claims of the present application regarding a mobile terminal and server into Schneier regarding its disclosure of Alice and Bob (the Examiner asserting that Alice is a mobile terminal and Bob is a server). Moreover, the limitations in the claims of the present application relate to use in a wireless local area network (WLAN). The Examiner admits that none of the RFC documents nor Schneier disclose or suggest wireless local area networks. The Examiner states that it is understood that the protocols defined in the RFC documents may be implemented in any network that uses IP. However, this statement is simply conclusory and has no support if none of the RFC documents disclose or suggest anything related to wireless local area networks.

Moreover, Applicants submit that one of ordinary skill in the art would have no motivation to combine Schneier (that simply relates to authentication protocols using certificates and a public key) with the RFC documents (all of which relate in some

way to the Internet). For example, RFC 2402 fully discloses an IP authentication header. If one uses this header to transfer information across the Internet, there is no need for the authentication framework disclosed in Schneier, that uses certificates and keys. One of ordinary skill in the art would have no motivation to combine Schneier with the RFC documents in an attempt to achieve the claimed invention.

Regarding claims 2-11 and 13-17, Applicants submit that these claims are dependent on one of independent claims 1 and 12 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. For example, Applicants submit that none of the cited references disclose or suggest the data packets being transferred from the mobile terminal to the access point using WLAN link level encryption in addition to the IPsec encryption, or where the WLAN link level encryption comprises WEP encryption.


Accordingly, Applicants submit that Schneier does not disclose or suggest the limitations in the combination of each of claims 1-17 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

In view of the foregoing amendments and remarks, Applicants submit that claims 1-17 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested.

U.S. Application No. 09/502,567

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (referencing attorney docket no. 0173.38045X00).

Respectfully submitted,  
ANTONELLI, TERRY, STOUT & KRAUS, LLP



---

Frederick D. Bailey  
Registration No. 42,282

FDB/sdb  
(703) 312-6600